学校编码：10384　　分类号_____密级_____
学　　号：X2009230260　　UDC _____

厦门大学

硕 士 学 位 论 文

医院网络可视化入侵检测系统设计与实现

Design and Implementation of the Visualized Intrusion Detection System of a Hospital Network

刘懿萱

指导教师姓名：廖明宏　教授

专　业　名　称：软 件 工 程
论文提交日期：2011 年 4 月
论文答辩时间：2011 年 5 月
学位授予日期：2011 年　月

答辩委员会主席：_____
评　　阅　　人：_____

2011 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

网络技术和电子技术的快速发展，积极推动了各行各业的信息化和网络化发展，给企业、政府、学校、医院等众多的单位带来了工作便利。同时，也使得各个单位的网络建设越来越庞大，本文主要针对医院网络进行研究。医院的网络环境比较复杂，一般都拥有成千上万的网络用户，而医院的网络管理相对松散，这给网络安全问题带来更多的隐患。通常情况下，医院网络会受到外界的攻击，有时也有来自网内的攻击，对于医院网络的这些不安全的问题，必须采用积极的措施避免和克服医院网络面临着的隐患，确保整个医院网络的安全，这样才能保证医院的工作正常进行，不至于由于网络问题给工作带来严重的影响。

本文首先分析了入侵检测系统的相关概念，在理论分析后提出了目前医院环境中 Web 系统存在的问题和医院网络环境中使用可视化入侵检测系统的重要性。然后对医院网络可视化入侵检测系统进行了需求分析，总结了医院可视化入侵检测系统的特点、功能和性能。最后结合某医院具体案例，提出了可视化入侵检测系统在医院网络的设计和实现。首先通过对某医院网络现状分析，找出存在问题，接着提出了设计的大体思路，最后结合设计思想，提出了某医院可视化入侵检测系统在医院网络中对于数据采集、安全响应、数据绘制与显示、可视化查询和异常检测等功能的具体实现。

关键词：医院网络；入侵检测；可视化；网络安全

ABSTRACT

Network technology and the rapid development of electronic technology, and actively promote the industries of information technology and network development, to corporate, government, schools, hospitals and other units to bring the working facilities. It also makes the construction of the various units of an ever-growing network of networks, this study focused on the hospital network. Hospital's network environment is complex and usually have tens of thousands of Internet users, and the hospital is relatively loose network management, network security issues that bring more to the hidden dangers. Typically, hospitals outside the network will be attacked, and sometimes the attack from the net, for the hospital network, these problems of insecurity, must be positive measures to avoid and overcome the risks facing the hospital network to ensure that the entire hospital network security, so as to ensure the hospital's normal, and will not work because of network problems to serious repercussions.

This article analyzes the concepts of intrusion detection system, made in the theoretical analysis of the current hospital environment, the problems in the Web system and hospital network environment using the visual importance of intrusion detection systems. Visualization of the hospital network and intrusion detection system needs analysis, summarizes the visual intrusion detection system, the hospital features, functions and performance. Finally, the specific case of a hospital, made a visual intrusion detection system in the hospital network design and implementation. First through the network status of a hospital network analysis to identify problems and then propose the design of the general idea, and finally with design ideas, put forward a hospital visual intrusion detection system network in the hospital network for data collection, security response, Data mapping and display, query and visualization functions such as anomaly detection implementation.

Keywords: Hospital network; Intrusion detection; Visualization; Network security

目 录

CONTENTS

第一章 引言

1.1 课题的研究背景

当前，网络技术的快速发展，促进了网络规模的不断扩大，使得网络规模不断升级。我国医院在网络快速发展的同时，为了更好的实现知识共享，提高办公效率，在医院内都进行网络了信息化建设，并且建立了自己的办公自动化和信息化网络平台，医院网络建设的同时积极带动了医院的发展。目前，计算机网络已经成为医院必不可少的基础硬件设施。同时由于接入 Internet 所带来的安全问题给医院网络管理者带来了极大的挑战，随处可得的黑客工具和不断曝光的系统漏洞使网络攻击随处可在。

医院网络系统是一个非常庞大而复杂的系统，它不仅要为现代化医院办公、综合信息管理和办公自动化等一系列应用提供一个基本环境（平台），还要为各种应用系统提供多种 Internet 服务，如 DNS、WWW、E-mail、FTP、数据库以及视频点播和视频会议等。为此，医院网络的安全问题也就变得日益突出。医院网络的安全对维护医院的正常的办公秩序，保证医院网络资料等起着极为重要的作用。不过，在现实的生活中，医院网络经常受到内部外部的攻击和入侵，使得医院网络的安全很不乐观，入侵事件在医院网络中经常发生，给医院的办公带来了很大的影响。因此，为了更好的促进医院正常办公，确保内外正常交流、医院网络的安全问题受到了领导和很多网络专家关注的重要问题。

在医院网络中遇到最典型的网络攻击是以大量的端口扫描等手段获取关于攻击对象的信息为开端的，这个过程必然产生大量的异常网络流量，预示着即将到来的真正攻击，然而当前被广泛使用的网络产品都有一个普遍的弱点就是被动防御，也就是说对大量异常网络流量这种重要的网络攻击前兆无法去检测、分析，错过了最佳的防御时机。要变被动为主动，这就要求网管人员对网络的运行状态进行实时监控以便随时发现入侵征兆并进行具体分析，然后及时进行干预，从而取得防患于未然的效果。完成这种功能的安全产品就是入侵检测系统(Intrusion Detection Systems, IDS)。

很多医院都建立了自己的网络，随着医院规模的不断扩大，医院网络也在不断的升级，网络安全问题也摆在面前，为了更好保证医院正常办公，医院一般都

投资建立大型医院内部外部结合的网络。目前，医院的网络安全仅靠单纯的防火墙策略已经无法满足当前的需要，网络的防卫必须采用一种纵深的、多样的手段。在这种环境下，入侵检测技术成为了网络信息安全领域研究的重点和热点。

1.2 国内外研究现状

随着计算机技术和网络技术的飞速发展，在现代建设中的应用越来越广泛，网络建设的热情在我国各行各业空前高涨。医院网络的普及，为合理配置医院资源，充分利用网络资源提供了可能。目前，医院网络已经应用到了医院办公、学习、交流的各个领域，如医生的办公，医院的活动安排以及医院的其它管理部门等等。医院网络在医院的正常办公领域中发挥着越来越重要的作用同时，自身的安全也成为了一个极为重要的问题。

当前，针对医院网络的攻击事件是频频发生，严重影响到医院的各项活动的正常运行。针对医院网络的攻击主要来自两个方面：一是来自外部公网的攻击，另一方面是来自内部网络的攻击。对于大型医院网络而言，由于其内部用户众多，来自内部的攻击或通过控制内部主机而实现对外攻击的现象往往占有很高的比例，而造成的破坏性大大超过外部攻击。

基于医院网络自身的特点，造成医院网络入侵的原因包括：(1)医院网络的宽带和大量主机资源，为黑客发动攻击提供了较好的环境条件；(2)医院网络内部交往比较频繁，内部相互开放，很多服务器可以自由访问，安全度很低，黑客很容易隐藏身份；(3)很多医院提供了外部访问服务，这样就为黑客网络中进行入侵提供了窗口；(4)医院网络中主机和网络设备通常没有可靠的安全系统，很容易受到攻击和入侵。

目前，对于入侵检测研究很多，主要有开放性、带宽高、主机多的特点，因此医院网络就成了许多比较严重的网络攻击事件中的主阵地，例如 2002 年黑客造成的 Yahoo 和 EBay 等网站服务一度关闭的拒绝服务攻击，据调查就是以学校为基地从校园网络中发起的。当然，更多的入侵者是乐于以攻击网络为目标，尤其是在攻击者处于“练手”的实验阶段。而作为互联网的一种主要的存在方式和组成部分，从某种意义上说局域网的安全问题几乎反映了所有的网络安全问题。

对于网络的入侵和攻击，最常用的防范方法就是采用防火墙(Firewall)。防火墙技术目前比较成熟，他被运用在各种不不同的网络或者被用在网络安全域

上。防火墙在网络安全运用中，被运用在网络层，它的作用就是通过防火墙来保护与医院网络相连的整个内部网络安全或单独节点安全。防火墙使用起来简单实用，并且具有较高透明度，并且使用防火墙技术时，可以在不破坏原有网络应用系统的基础上实现一定的安全。不过，防火墙技术在运用过程中，也面临着自身的弱点，就是防火墙技术是一种被动的防御性技术，在网络安全防御过程中，如果只使用防火墙技术是不行的，这种被动的网络安全技术给医院的网络带来了隐患。因为网络破坏者可以可以找到防火墙的漏洞，避开防火墙，来实现对医院网络的攻击。同时，防火墙技术在运行过程中，对来自医院内部的攻击也束手无策。防火墙技术使用过程中，服务方式单调，不是拒绝，就是通过，而医院网络运行中，所受到的攻击大部分来自医院外部，显然如果只采用防火墙技术就很难保证整个医院的网络安全。为了更好的确保医院网络安全，通常就利用入侵检测技术作为辅助，这样可以更好的维护医院网络安全。入侵检测技术是一种积极主动的网络安全防御技术，入侵检测技术可以积极的防御内部攻击、也可以有效的对付外部攻击和误操作，有效的对网络安全进行实时保护。入侵检测技术的主动性防御，受到医院的青睐，木器很多的医院在网络安全管理中都采用了入侵检测技术。

国内外对入侵检测技术的研究有很多。目前，有对分布式网络环境下的入侵检测技术和入侵检测代理技术的研究。但是对可视化入侵检测技术，特别是可视化入侵检测技术在医院网络中研究很少。入侵检测系统中采用信息可视化可以更好的提高效率，通过人机交互手段，对于网络入侵和网络攻击有效快速的处理。

例如，在医院网络建设中，一般都有专门的服务器，实现资源共享。而入侵者在入侵过程中如果采用非法的代理服务器访问医院资源，这种行为将会被入侵检测系统检测后阻拦，因为这是是一种入侵行为；而入侵者如果通过合法的代理服务器访问医院的服务器资源，则入侵检测技术就视为正常行为。不过，普通自动化的入侵检测系统在用户区分上，对于代理服务器访问的攻击者无法识别，也不能确认该次访问的合法性。而采用可视化入侵检测系统，网络安全管理员就可根据可视化页面，对访问者或入侵者进行快速有效的识别，进而轻易区分出该次访问是否合法。

1.3 研究内容及意义

目前大多数网络安全产品都以安全日志的方式记录系统安全状态。网络分析

人员通常通过监视和分析相应的日志信息，找出可疑事件作进一步诊断，最后对确定的异常和攻击做出回应。对于入侵检测系统，该日志则是以警报文件形式进行存储。在一个大规模网络下入侵检测系统一般一天就会产生数百万条警报，如果网络分析人员使用传统的逐条警报分析的方法显然无法在有限时间内处理全部警报信息。而往往这些警报大多是重复或误报。因此也成为了入侵响应的瓶颈之一。另一方面，由于分析人员关注的常常是单一的警报数据，缺乏对网络整体状态信息的了解，使其很难识别一些大规模、协作式和周期漫长的网络攻击事件。此外，当前入侵检测系统配置越来越复杂、规则库越来越庞大，未经过长期专业训练或拥有丰富安全管理经验的人很难仅凭一些警报信息发现隐含的攻击行为和入侵过程，也就无法对攻击意图和趋势做出预测或者提前进行防范。

基于对以上问题的考虑，人们开始将可视化技术引入到网络安全领域。对于大量的安全数据和日志信息的分析处理，如果可以将网络数据以图形图像的方式表现出来，那么利用人们的视觉功能处理这些大量数据信息，就会使分析过程加快和大大简化。

针对目前医院网络安全所面临的问题，本文主要采用建立可视化入侵检测系统来进行防御。在可视化入侵检测系统时，采用人机接口向网络管理人员直接提供可视化的信息，这样可以让网络管理人员更好的感知计算机系统中的数字信息，大大提高了网络管理者与计算机之间的信息交流，并且带动整个入侵检测系统的检测效率。可视化入侵检测系统可以把网络监控信息进行可视化应用，并且通过计算机处理，直接向安全专家与网络安全管理人员提供直观的可视化的用户操作界面，这样就大大加强了检测过程中安全专家和网络安全管理员与系统之间的交互，可以减少误报率，大大提高了整个入侵检测系统的性能。因此，医院建立可视化入侵检测系统对医院的网络安全来说，是可行的，也是非常重要的。

1.4 论文章节安排

本文研究共分为五章，各章主要内容如下：

第一章，绪论。主要说明本文的选题背景与意义、相关文献综述、研究内容章节安排。

第二章，入侵检测技术的理论研究。主要分析入侵检测技术的概念、分类和目前存在的问题及入侵检测技术的发展方向。

第三章，对某医院可视化入侵检测系统进行需求分析。这章主要分析某医院网络的现状，以及建立可视化入侵检测系统的必要性和可行性。

第四章，提出某医院可视化入侵检测系统总体设计。通过安全需求、功能实现、模型建立三个方面进行了说明。

第五章，提出某医院可视化入侵检测系统的设计与实现。主要对提出某医院可视化入侵检测系统中的数据采集、安全响应、数据绘制与显示、可视化查询和异常检测五大模块进行了说明，最后为了更好的说明某医院可视化入侵检测系统的可行性和实用价值，进行了系统测试并对测试结果进行了分析。

第二章 入侵检测技术理论研究

2.1 入侵检测系统的概述

2.1.1 入侵检测系统的概念

入侵检测系统(Intrusion Detection Systems 简称：IDS)是一种主动防御系统，这个系统首先运用计算机技术对网络传输中的若干关键点进行信息收集，接着对这些收集来的信息进行分析，目的是查出有违反安全策略的行为或者检测攻击的行为，最后给予这些破坏行为给予一定的处理[1]。

入侵行为是计算机网络中的攻击行为，它主要是指入侵者或者网络破坏者对网络系统资源进行非授权使用，这种越权使用可能给别人的信息资源造成数据的破坏或丢失，或者造成系统对合法用户的服务请求阻止，使得整个系统瘫痪等等[2]。入侵检测技术就是为了入侵行为进行有效的检测，确保计算机系统的安全不受外界攻击和破坏而设计的一种可以及时发现网络入侵行为并把入侵行为及时报告给系统，入侵检测技术是一种用来对网络中的违反安全策略行为进行有效检测的技术。在网络传输中，违反计算机网络安全策略的行为主要有两种：一种是入侵行为，这种行为主要是非法用户进行的违规行为；另一种是滥用行为，这种行为是合法用户的违规行为[3]。入侵检测行为可以利用审计记录，有效的识别出计算机网络中的任何不合法的活动，并给予一定的限制和阻止，进而实现对计算机系统的安全保护。

入侵检测系统就是基于入侵检测技术而设计的一个对入侵行为进行检测的系统，它可以对入侵攻击在对系统破坏之前，对入侵攻击行为进行有效的检测，并听过报警机制与防护机制把系统中的入侵攻击行为进行驱逐；对于入侵进行中的攻击行为可以及时的阻止，入侵检测系统可以有效的减少入侵攻击，降低攻击对系统带来的损失和影响；对于攻击后破坏，可以收集到入侵攻击中的相关信息，这些信息对于以后的防范处理有着积极的作用，系统会主动把入侵攻击行为添加到知识库内，进而增强入侵检测系统的防范能力和保护能力。

常用的入侵检测方法有三种：专家检测、特征检测和统计检测，在使用过程中，并不是只用一种，有时可能三种都用，这样可以更好的对入侵行为进行检测。根据我国 09 年公安部计算机信息系统安全产品质量监督检验中心对我国网络入

侵的检测报告显示，我国送到产品质量监督检验中心检测的入侵检测产品中，有95%是属于使用入侵模板进行模式匹配检测产品，这些产品占了目前产品的主流，其他5%的产品是通过概率统计的方式进行统计检测的，这种产业有时结合日志的专家知识库系统进行匹配。

基于专家检测是入侵检测一般用在对有特征入侵行为进行检测。特征入侵是一定规律的入侵，这种入侵存在普遍性和共性，可以在不同的系统和不设置的网络中运用[4]。专家检测在使用前，首先要建立一个完备的知识库，这些知识库主要是对于以前的审计记录整理出来的，这些知识库建立不断的更新，具有一定的完备性与实时性。在系统实践中，一般采用把现有的入侵的知识转化为 if-then 结构，这样就可以采用条件语句为入侵检测特征，then 部分是入侵检测系统的防范措施。专家检测防范的效果完全取决于专家系统知识库的完备，如果专家系统知识库不完备，这样就无法保证对入侵行为进行系统的检测，加上入侵行为在不断更新，必须对专家系统知识库进行及时更新，这样才能确保系统检测的有效性，可以对最新的入侵行为进行有效的检测。

基于特征检测的入侵检测系统主要是对可以预知的入侵攻击或入侵方式给予确定性的描述，制订相应的事件检测模式，然后对入侵行为进行检测和防范。基于特征检测的入侵检测系统在运行过程中，遇到被审计的事件与事先预知的入侵事件模式相匹配时，就会发出报警提示。基于特征检测的方法在使用过程中预报检测的准确率较高，不过由于对未知的没有任何防范措施，这样在实施过程中对没有预测到的入侵与攻击行为显得素手无力，因此，也存在一定的局限性。

基于统计检测的入侵检测系统是对常用异常检测进行统计，统计的常用参数有：入侵攻击事件的审计数量、入侵攻击事件的时间间隔、系统的资源消耗情况等等。采用统计检测的方法可以在使用过程中，不断的“学习”用户的操作惯性，然后进行不断的统计整理，这样就可以提供较高的检出率与可用性。不过统计检测的方法也存在一定的局限性，因为这种方法“学习”能力有限，入侵者可以借“学习”的机会正常操作，通过逐步“训练”，进行入侵攻击，带有一定的隐患性。

2.1.2 入侵检测系统的原理和功能

1、入侵检测系统的原理

入侵检测系统工作过程中对于入侵检测通常有实时入侵检测和事后入侵检